

P23877.P07



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Atsushi MINEMURA

Appln No. : 10/602,639

Group Art Unit: 2131

Filed : June 25, 2003

Examiner: Unknown

For : DEVICE AUTHENTICATION SYSTEM

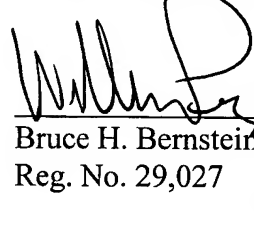
**SUPPLEMENTAL CLAIM OF PRIORITY
SUBMITTING CERTIFIED COPY**

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Further to the Claim of Priority filed June 25, 2003 and as required by 37 C.F.R. 1.55, Applicant hereby submits a certified copy of the application upon which the right of priority is granted pursuant to 35 U.S.C. §119, i.e., of Japanese Application No.2002-198719, filed July 8, 2002.

Respectfully submitted,
Atsushi MINEMURA


Bruce H. Bernstein
Reg. No. 29,027

September 25, 2003
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 7月 8日

出 願 番 号

Application Number:

特願2002-198719

[ST.10/C]:

[JP2002-198719]

出 願 人

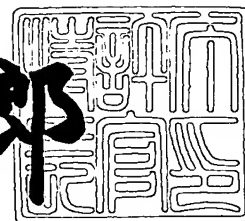
Applicant(s):

松下電器産業株式会社

2003年 6月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3050589

【書類名】 特許願

【整理番号】 2030744018

【提出日】 平成14年 7月 8日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 15/00

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 峰村 淳

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100099254

 【弁理士】

 【氏名又は名称】 役 昌明

【選任した代理人】

 【識別番号】 100100918

 【弁理士】

 【氏名又は名称】 大橋 公治

【選任した代理人】

 【識別番号】 100105485

 【弁理士】

 【氏名又は名称】 平野 雅典

【選任した代理人】

 【識別番号】 100108729

 【弁理士】

 【氏名又は名称】 林 紘樹

【手数料の表示】

【予納台帳番号】 037419

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9102150

【包括委任状番号】 9116348

【包括委任状番号】 9600935

【包括委任状番号】 9700485

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 機器認証システム

【特許請求の範囲】

【請求項 1】 第 1 の機器が第 2 の機器を認証する機器認証システムであって、

前記第 1 の機器は、
前記第 2 の機器と情報の送受信を行う送受信手段と、
第 1 の認証情報をセキュアな領域に保持する第 1 の情報保持手段と、
認証の判定を行う判定手段と、
を備え、

前記第 2 の機器は、
前記第 1 の機器と情報の送受信を行う送受信手段と、
第 2 の認証情報を保持する第 2 の情報保持手段と、
当該機器の外部から第 3 の認証情報を取得する情報取得手段と、
前記第 2 の認証情報と前記第 3 の認証情報とから第 4 の認証情報を生成し、前記
第 4 の認証情報を前記送受信手段を通じて前記第 1 の機器へ送出する認証情報生成手段と、
を備え、

前記判定手段は、前記第 1 の認証情報と前記第 4 の認証情報との適合性を判定することにより、前記第 2 の機器を認証する機器認証システム。

【請求項 2】 前記第 2 の認証情報が、前記第 2 の機器に固有な情報であることを特徴とする請求項 1 に記載の機器認証システム。

【請求項 3】 前記第 2 の認証情報が、前記第 1 の機器によって生成された任意情報であることを特徴とする請求項 1 に記載の機器認証システム。

【請求項 4】 前記第 2 の認証情報が、認証処理の都度更新され、前記第 2 の認証情報の更新に伴って、前記第 1 の機器の第 1 の情報保持手段で保持される前記第 1 の認証情報が更新されることを特徴とする請求項 3 に記載の機器認証システム。

【請求項 5】 前記第 1 の機器が前記第 1 の認証情報を保持していないとき

、前記第 1 の機器と相互認証した機器が、前記第 2 の機器から前記第 4 の認証情報を取得して、前記第 1 の機器に前記第 1 の認証情報を初期設定することを特徴とする請求項 1 に記載の機器認証システム。

【請求項 6】 前記第 3 の認証情報が、前記第 1 の機器と相互認証した機器により保持され、認証処理時に、前記機器から前記第 2 の機器に与えられることを特徴とする請求項 1 に記載の機器認証システム。

【請求項 7】 第 1 の機器が第 2 の機器を認証する機器認証方法であって、
前記第 1 の機器は、第 1 の認証情報をセキュアな領域に保持し、
第 2 の認証情報を保持する前記第 2 の機器は、前記第 2 の認証情報と前記第 2 の機器の外部から与えられる第 3 の認証情報とから第 4 の認証情報を生成し、
前記第 1 の機器は、前記第 1 の認証情報と前記第 4 の認証情報との適合判定により、前記第 2 の機器を認証することを特徴とする機器認証方法。

【請求項 8】 第 1 の機器から認証を受ける第 2 の機器であって、
前記第 1 の機器と情報の送受信を行う送受信手段と、
第 2 の認証情報を保持する情報保持手段と、
当該機器の外部から第 3 の認証情報を取得する情報取得手段と、
前記第 2 の認証情報と前記第 3 の認証情報とから第 4 の認証情報を生成し、前記第 4 の認証情報を前記送受信手段を通じて前記第 1 の機器へ送出する認証情報生成手段と、
を備えた第 2 の機器。

【請求項 9】 前記送受信手段は、前記第 1 の機器より任意情報を受信し、
前記認証情報生成手段は、前記任意情報を前記第 4 の認証情報によって暗号化し、
前記送受信手段を通じて前記第 1 の機器へ送出することを特徴とする請求項 8 に記載の第 2 の機器。

【請求項 10】 前記送受信手段は、前記第 1 の機器より任意情報を受信し、
前記認証情報生成手段は、前記第 4 の認証情報を前記任意情報によって暗号化し、
前記送受信手段を通じて前記第 1 の機器へ送出することを特徴とする請求項 8 に記載の第 2 の機器。

【請求項 1 1】 認証の処理に必要な情報の更新を制御する更新制御手段を備え、

前記第 1 の機器からの認証に成功した後、前記更新制御手段は、

前記第 2 の認証情報に替えて、前記任意情報を新たなる第 2 の認証情報として前記情報保持手段へ保持させ、また、

前記第 3 の認証情報と前記任意情報とから新たなる認証情報であるキー情報を生成し、前記キー情報を前記送受信手段を通じて前記第 1 の機器へ保持させる、ことを特徴とする請求項 8 から 1 0 のいずれかに記載の第 2 の機器。

【請求項 1 2】 第 2 の機器を認証する第 1 の機器であって、

前記第 2 の機器と情報の送受信を行う送受信手段と、

第 1 の認証情報をセキュアな領域に保持する情報保持手段と、

前記送受信手段により受信した第 4 の認証情報と前記第 1 の認証情報との適合性を判定する判定手段と、
を備えた第 1 の機器。

【請求項 1 3】 任意情報を生成し、前記送受信手段を通じて前記第 2 の機器へ送出する任意情報生成手段を備え、

前記判定手段は、前記送受信手段により受信した情報を前記第 1 の認証情報によって復号し、復号された情報と前記任意情報との適合性を判定することを特徴とする請求項 1 2 に記載の第 1 の機器。

【請求項 1 4】 任意情報を生成し、前記送受信手段を通じて前記第 2 の機器へ送出する任意情報生成手段を備え、

前記判定手段は、前記送受信手段により受信した情報を前記任意情報によって復号し、復号された情報と前記第 1 の認証情報との適合性を判定することを特徴とする請求項 1 2 に記載の第 1 の機器。

【請求項 1 5】 前記第 2 の機器の認証に成功した後、

前記情報保持手段は、前記第 1 の認証情報に替えて、前記送受信手段により受信した新たなる認証情報であるキー情報を新たなる第 1 の認証情報として保持することを特徴とする請求項 1 2 から 1 4 のいずれかに記載の第 1 の機器。

【請求項 1 6】 第 1 の機器から認証を受ける第 2 の機器に内蔵されたコン

ピュータに、

当該機器が保持する第 2 の認証情報と当該機器の外部から取得した第 3 の認証情報とから第 4 の認証情報を生成する手順と、

前記第 1 の機器に任意情報の発行を要求する手順と、

前記第 1 の機器より受信した前記任意情報を前記第 4 の認証情報によって暗号化して前記第 1 の機器へ送出する手順と、

を実行させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、機器間において認証を行う機器認証システムと、その認証方法と、その方法を実施する機器と、機器の動作を規定するコンピュータプログラムに関し、特に、認証キーの格納に必要なセキュア領域を持たない機器に対する外部認証を可能にするものである。

【0002】

【従来の技術】

エンティティ（相手）認証は、従来から、通信相手が本人であることを確認したり、ファイル共有サービスを提供しているコンピュータが、接続要求するユーザについて、アクセス権限を与えるべき正当なユーザであることを確認したりするために行われている。

【0003】

相手認証には種々の方式が存在している。その一つであるチャレンジ／レスポンス方式では、例えば、両方の当事者 A、B が秘密に保持する対称鍵を所持し、一方の当事者 A は乱数（チャレンジ）を生成して他方の当事者 B に渡し、他方の当事者 B は、対称鍵を使ってその乱数を暗号化した値（レスポンス）を当事者 A に返す。当事者 A は、対称鍵を用いてレスポンスを復号化し、レスポンスとチャレンジとの関係に矛盾がなければ正当な相手と認識する。

【0004】

また、近年、CPU や暗号処理用のコプロセッサが内蔵されたメモリデバイス

との間で相互認証処理を行う書き込み／読み込み制御用マイコンが開発、市販されている。このマイコンはメモリデバイスの書き込み／読み込みを制御するコントローラを内蔵し、このマイコンを搭載した機器の下で、その機器に装着されるメモリデバイスとの間で相互認証を実行する。

【 0 0 0 5 】

【発明が解決しようとする課題】

最近、インターネット対応の携帯電話機にメモリデバイスを装着し、携帯電話機を通じてサービスサーバから取得した音楽や画像、ゲームソフト等のコンテンツをメモリデバイスに蓄積する方式が検討されている。

この場合、メモリデバイスに蓄積されたデータが、そのデータをダウンロードした携帯電話機以外では利用できないように、メモリデバイスの利用可能な携帯電話機を特定化しようとする考え方がある。これは、携帯電話事業者が、コンテンツ配信サービスを、情報料を課金する契約者の携帯電話機に限ることにより、競合他社との差別化を図り、契約数の拡大を図るためである。

【 0 0 0 6 】

メモリデバイスの利用を特定の携帯電話機だけに限定することは、メモリデバイスが携帯電話機を相手認証し、該当する携帯電話機で無いときに、携帯電話機との応答を拒否すれば可能になる。

しかし、ＩＣチップが埋め込まれているメモリデバイスやＩＣカードなどのセキュアデバイスは対称鍵を秘密裏に保持できるが、セキュアな領域を持たない携帯電話機は、対称鍵を秘密に保持することができない。

また、この携帯電話機に、前述するメモリデバイスとの相互認証処理を行うマイコンを搭載することは、携帯電話機の小型・薄型化を損ない、コストが高くなると言う問題点がある。

【 0 0 0 7 】

本発明は、こうした問題点を解決するものであり、セキュアな領域を持たない機器を相手とする認証を安全確実に行うことができる機器認証システムを提供し、また、その認証方法と、その方法を実施する機器と、その動作を規定するコンピュータプログラムとを提供することを目的としている。

【0008】

【課題を解決するための手段】

そこで、本発明では、第1の機器が第2の機器を認証する機器認証システムにおいて、第1の機器に、第2の機器と情報の送受信を行う送受信手段と、第1の認証情報をセキュアな領域に保持する第1の情報保持手段と、認証の判定を行う判定手段とを設け、第2の機器に、第1の機器と情報の送受信を行う送受信手段と、第2の認証情報を保持する第2の情報保持手段と、当該機器の外部から第3の認証情報を取得する情報取得手段と、第2の認証情報と第3の認証情報とから第4の認証情報を生成し、この第4の認証情報を送受信手段を通じて第1の機器へ送出する認証情報生成手段とを設け、判定手段が、第1の認証情報と第4の認証情報との適合性を判定して第2の機器を認証するように構成している。

【0009】

また、本発明では、第1の機器が第2の機器を認証する機器認証方法において、第1の機器は、第1の認証情報をセキュアな領域に保持し、第2の認証情報を保持する第2の機器は、この第2の認証情報と第2の機器の外部から与えられる第3の認証情報とから第4の認証情報を生成し、第1の機器が、第1の認証情報と第4の認証情報との適合判定により、第2の機器を認証するようにしている。

【0010】

また、本発明では、第1の機器から認証を受ける第2の機器に、第1の機器と情報の送受信を行う送受信手段と、第2の認証情報を保持する情報保持手段と、当該機器の外部から第3の認証情報を取得する情報取得手段と、第2の認証情報と第3の認証情報とから第4の認証情報を生成し、この第4の認証情報を送受信手段を通じて第1の機器へ送出する認証情報生成手段とを設けている。

【0011】

また、本発明では、第2の機器を認証する第1の機器に、第2の機器と情報の送受信を行う送受信手段と、第1の認証情報をセキュアな領域に保持する情報保持手段と、送受信手段により受信した第4の認証情報と第1の認証情報との適合性を判定する判定手段とを設けている。

【0012】

また、本発明のコンピュータプログラムでは、第 1 の機器から認証を受ける第 2 の機器に内蔵されたコンピュータに、当該機器が保持する第 2 の認証情報と当該機器の外部から取得した第 3 の認証情報とから第 4 の認証情報を生成する手順と、第 1 の機器に任意情報の発行を要求する手順と、第 1 の機器より受信した任意情報を第 4 の認証情報によって暗号化して第 1 の機器へ送出する手順とを実行させることを規定している。

【 0 0 1 3 】

そのため、第 2 の機器に保持された認証情報（第 2 の認証情報）と、例えばユーザが入力する識別情報（第 3 の認証情報）とから新たな認証情報（第 4 の認証）が生成され、この新たな認証情報と、第 1 の機器のセキュアな領域に保持された認証情報（第 1 の認証情報）との適合性が判定されるため、第 1 の機器は、セキュアな領域を持たない第 2 の機器を相手とする認証を安全確実に行うことができる。

また、第 1 の機器がメモリデバイスであり、第 2 の機器が携帯電話機である場合、この認証処理により、メモリデバイスに蓄積されたデータの利用を特定の携帯電話機だけに限定することができる。

【 0 0 1 4 】

【発明の実施の形態】

本発明の機器認証システムでは、チャレンジ／レスポンス方式により機器 A が機器 B を認証する。

図 1 に示すように、機器 A 80 は、機器 B 90 と情報の送受信を行う送受信手段 84 と、第 1 の認証情報をセキュアな領域に保持する情報保持手段 81 と、送受信手段 84 により受信した認証用の情報（第 4 の認証情報）と第 1 の認証情報との適合性を判定する判定手段 82 と、乱数等の任意情報を生成する任意情報生成手段 83 とを備えており、一方、機器 B 90 は、機器 A 80 と情報の送受信を行う送受信手段 91 と、第 2 の認証情報を保持する非セキュアな情報保持手段 94 と、機器 B 90 の外部から第 3 の認証情報を取得する情報取得手段 95 と、第 2 の認証情報と第 3 の認証情報とから認証用の情報（第 4 の認証情報）を生成し、この第 4 の認証情報を送受信手段 91 を通じて機器 A 80 へ送出する認証情報生成手段 93 と、情報保持手段 94 で

保持された第 2 の認証情報を更新する更新制御手段92とを備えている。

【 0 0 1 5 】

このシステムでは、認証を受ける機器 B 90 が、認証情報生成手段93により、情報保持手段94で保持する第 2 の認証情報と、情報取得手段95により機器 B 90 の外部から取得した第 3 の認証情報とから認証用の情報（第 4 の認証情報）を生成する。機器 B 90 は、第 4 の認証情報を生成すると、機器 A 80 に任意情報の発行を要求する。

この要求を受けた機器 A 80 は、任意情報生成手段83で乱数等の任意情報を生成し、機器 B 90 に送出する。

【 0 0 1 6 】

機器 B 90 は、機器 A 80 より受信した任意情報を第 4 の認証情報によって暗号化して機器 A 80 へ送出する。

機器 A 80 は、判定手段82により、機器 B 90 から受信した情報を情報保持手段81で保持する第 1 の認証情報で復号化し、復号された情報と機器 B に与えた任意情報との一致を検証して、第 1 の認証情報と第 4 の認証情報との適合性を判定する。適合性が認められれば、機器 B 90 を認証する。

【 0 0 1 7 】

機器 B 90 では、認証に成功した場合に、更新制御手段92が、機器 A 80 から受信した任意情報を次回認証時の第 2 の認証情報として、情報保持手段94に保持させる。また、この任意情報と第 3 の認証情報とから新たな認証情報であるキー情報を生成し、このキー情報を送受信手段91を通じて機器 A 80 に送る。機器 A 90 は、このキー情報を次回認証時の第 1 の認証情報として、セキュアな情報保持手段81で保持する。

なお、このシステムにおいて、機器 B 90 が機器 A 80 を認証することは任意である。

【 0 0 1 8 】

以下、認証する機器 A がメモリデバイスであり、認証される機器 B が携帯電話機である場合の実施形態について説明する。この機器認証システムでは、チャレンジ／レスポンス方式によりメモリデバイスと携帯電話機との相互認証が行われ

る。このチャレンジ／レスポンス方式における共通鍵（キー）は、ユーザが入力する識別情報と、携帯電話機に格納されたデータとから動的に生成される。

【 0 0 1 9 】

図 2 は、新しいメモリデバイス 10 が携帯電話機 20 に装着されたときに、メモリデバイス 10 を発行したサービスサーバ 30 により、チャレンジ／レスポンス方式のキー 12 がメモリデバイス 10 に初期設定される手順を示している。

メモリデバイス 10 は、例えば、図 4 に示すように、サービスサーバ 30 からダウンロードされるコンテンツを格納する、フラッシュメモリ等から成るメモリ 41 と、メモリ 41 へのデータの書き込み／読み出しを制御する、耐タンパ性を有するメモリコントローラ 42 とを備えており、メモリコントローラ 42 は、メモリデバイス 10 の動作を制御する CPU 43 と、CPU 43 が作業領域として使用する RAM 44 と、CPU 43 の動作を規定するプログラムが格納された ROM 45 と、EEPROM 等から成る耐タンパ性を有する内部不揮発性メモリ 46 と、CPU 43 から任された暗号処理等の演算処理を行う暗号コプロセッサ 47 と、携帯電話機 20 との間でデータを入出力する入出力部（I/O）48 と、メモリ 41 との間の I/O 49 とを備えている。

【 0 0 2 0 】

また、携帯電話機 20 は、例えば、図 5 に示すように、メモリデバイス 10 が装着されるメモリデバイススロット 51 と、アンテナ 56 を通じてサービスサーバ 30 と通信を行う無線通信部 57 と、携帯電話機 20 の動作を制御する CPU 52 と、CPU 52 の動作を規定するプログラムが格納される ROM 53 と、チャレンジ／レスポンス方式のキーを生成するためのデータが書き込まれる EEPROM 54 と、液晶表示画面（LCD）55 と、マイク 58 やスピーカ 59 の音声処理部 60 と、スイッチ 61 のキー制御部 62 とを備えている。

【 0 0 2 1 】

また、サービスサーバ 30 は、例えばコンテンツ配信サービスを実施するサービス提供会社の公式サイトである。サービス提供会社が運営するサービスサーバ 30 は、電話会社のキャリアゲートウェイ（GW）31 に接続しており、このキャリア GW 31 により、サービスサーバ 30 に中継される携帯電話機 20 の電話番号が真正で

あることが保証される。換言すれば、サービス提供会社と契約した携帯電話機20で無いと公式サイトのサービスサーバ30にアクセスすることはできない。

【 0 0 2 2 】

さて、図2において、メモリデバイス10は、サービスサーバ30の公開鍵11と、メモリデバイスの秘密鍵13とが耐タンパ性の内部不揮発性メモリ46に格納された状態で、サービスサーバ30を運営するサービス提供会社から発行される。

また、携帯電話機20は、EEPROM54に製造番号21が格納され、また、相互認証の動作を規定するアプリケーション22がROM53に格納されている。

【 0 0 2 3 】

メモリデバイス10を携帯電話機20のメモリデバイススロット51に装着すると、メモリデバイス10と携帯電話機20との相互認証が行われるが、メモリデバイス10に相互認証用の情報が未設定である場合には、携帯電話機20がサービスサーバ30に接続して、メモリデバイス10に相互認証用の情報を初期設定する処理が次の手順で行われる。

- ①サービス提供会社がメモリデバイス10を発行する。
- ②ユーザが、相互認証用の情報が未設定のメモリデバイス10を携帯電話機20に装着すると、
- ③携帯電話機20のアプリケーション22は、キャリアGW31を通じてサービスサーバ30に接続し、メモリデバイス10とサービスサーバ30との相互認証を求める。

【 0 0 2 4 】

④サービスサーバ30は、チャレンジ（乱数）の発行を指示するGetchallenge（動的情報発行命令）をメモリデバイス10に送る。この命令は、携帯電話機20をスルーしてメモリデバイス10に直接送られる。メモリデバイス10は、その命令に従ってチャレンジ（乱数）を生成し、サービスサーバ30に送る。サービスサーバ30は、乱数をサーバ秘密鍵で暗号化してレスポンスを生成し、これをサービスサーバ30の認証を指示するExternalAuthenticate（外部認証命令）とともにメモリデバイス10に送信する。メモリデバイス10は、暗号化されている乱数をサーバ公開鍵11で復号化し、レスポンスとチャレンジとの関係に矛盾がなければサービスサーバ30を正当な相手と認証する。また、メモリデバイス10とサービスサーバ30は、

立場を逆にしてこれと同じ手順を行い、サービスサーバ30が、メモリデバイス10を認証する。この時にはメモリデバイス10の秘密鍵13を利用する。相互認証が完了すると、サービスサーバ30とメモリデバイス10との間でセキュアメッセージングを用いて秘匿通信路を生成する。

【 0 0 2 5 】

- ⑤サービスサーバ30は、アプリケーション22にキーの生成を指示する。
- ⑥これを受けて、アプリケーション22は、液晶表示画面（LCD）55を通じてユーザに識別情報の入力指示を出す。
- ⑦ユーザが識別情報を入力すると、アプリケーション22は、製造番号21と識別情報とからキーを生成し、サービスサーバ30に送信する。
- ⑧サービスサーバ30は、携帯電話機20から得たキーをメモリデバイス10に送信する。メモリデバイス10は、このキー情報を受け入れて、耐タンパ性の内部不揮発性メモリ46に格納する。

こうして、メモリデバイス10にキー12が初期設定される。このキー12は、携帯電話機20の製造番号とユーザの頭の中にある識別情報とから生成されているので、他人が携帯電話機20に格納された製造番号を知ったとしても、同じキー12を生成することはできない。

【 0 0 2 6 】

次に、キー12が設定されたメモリデバイス10を携帯電話機20に装着したときに、メモリデバイス10と携帯電話機20との間で行われる相互認証の手順について説明する。

図3に示すように、

- ①ユーザがメモリデバイス10を携帯電話機20に装着する。
- ②アプリケーション22は、液晶表示画面（LCD）55を通じてユーザに識別情報の入力指示を出す。
- ③ユーザが識別情報を入力すると、アプリケーション22は、製造番号21と識別情報とからキーを生成する。
- ④アプリケーション22は、メモリデバイス10にGetchallengeを発行する。これを受けたメモリデバイス10は、challenge用乱数を生成してアプリケーション22に

送り、アプリケーション22は、これを取得する。

⑤アプリケーション22は、取得したchallenge用乱数を③で生成したキーで暗号化する。

【 0 0 2 7 】

⑥次に、アプリケーション22は、メモリデバイス10にExternalAuthenticateを発行し、⑤で暗号化したchallenge用乱数を渡す。

⑦メモリデバイス10は、暗号化されているchallenge用乱数を、キー12を用いて検証する。ここで、検証とは、キー12を用いて復号を行い、復号によって得られた情報（challenge用乱数）とメモリデバイス10が生成・保持しているchallenge用乱数との適合性を判定（主に一致の有無を確認）する処理であり、適合（一致）していれば認証成功となる。認証（外部認証）に成功すれば、携帯電話機20のアクセスを許可する。なお、ここで、“一致”とは、判定する対象の全bitの一致だけでなく、完全一致でない場合でも、上位／下位／中位の任意のビット数が一致していれば適合性有りとする、適合性判定・一致判定に関する公知の手法を広く含むものである。

また、メモリデバイス10と携帯電話機20は、立場を逆にして、携帯電話機20で乱数を生成し、これを暗号化する。これをメモリデバイス10に送り、メモリデバイス10は保持している秘密鍵でこれを復合化し、携帯電話機20に送り返す。携帯電話機20では、これが自ら生成した乱数と一致するかどうかを判定することで認証を行う。

【 0 0 2 8 】

⑧アプリケーション22は、⑦の外部認証が成功すると、④で取得したchallenge用乱数23をEEPROM54に格納する。この乱数23は次回の相互認証において製造番号21の代わりに使用される。

⑨アプリケーション22は、EEPROM54に格納したこの乱数23と識別情報とからキーを生成して、メモリデバイス10内に書き込む。メモリデバイス10は、このキー情報が認証した相手から送られて来たものであるため、それを受け入れて、耐タンパ性の内部不揮発性メモリ46に格納する。このキー12は次回の相互認証で使用される。

メモリデバイス10は、⑦において、外部認証に失敗した場合には、携帯電話機20のアクセスを拒否し、動作を停止する。

【 0 0 2 9 】

このように、この機器認証システムでは、携帯電話機20に格納された情報と、ユーザが入力した識別情報とを用いて動的にキーが生成され、初期設定後は、このキーを用いて、オフラインでメモリデバイス10と携帯電話機20との相互認証が行われる。そのため、セキュア領域を持たない携帯電話機20にはキーそのものが保持されないので、携帯電話機20から不正にキー情報が読み出される事態を回避することができる。

【 0 0 3 0 】

また、初回の相互認証のキーが携帯電話機20の固有情報を用いて生成されるため、メモリデバイス10の使用可能な機器は、その固有情報を有する携帯電話機20に限定される。

また、2回目以降の相互認証では、前回の相互認証に用いたchallenge用乱数と、ユーザにより設定された識別情報とから生成されたキーが用いられるので、キーが相互認証ごとに毎回変わり、また、携帯電話機20で保持するキー生成用の数値も相互認証ごとに毎回変わることになる。そのため、携帯電話機20とメモリデバイス10との間で交わす情報を盗み見るコピー攻撃を受けた場合でも、識別情報が解読される虞れは無く、また、携帯電話機20に保持された数値が盗み見られたとしても、何の問題もない。従って、不正に対して高い安全性を保つことができる。

【 0 0 3 1 】

なお、ここでは、メモリデバイス10と携帯電話機20とが相互認証する場合について示したが、メモリデバイス10のみが携帯電話機20を認証する片側認証であっても良い。

また、ここでは、携帯電話機20の固有情報として製造番号を用いる場合について説明したが、電話番号を使用しても良い。

【 0 0 3 2 】

また、ここでは、携帯電話機が、メモリデバイスから与えられた乱数をキーで

暗号化する場合について示したが、逆に、キーを乱数で暗号化してメモリデバイスに渡すようにしても良い。この場合でも、メモリデバイスは乱数を知っているので、復号化によりキーを取り出し、自ら保持しているキーと照合して携帯電話機を認証することができる。

また、メモリデバイス10は、非接触型 I C カード、接触型 I C カード、S D カード、MMC（マルチメディアカード）等のセキュア領域を持つ記録媒体が対象となる。

【 0 0 3 3 】

また、この機器認証システムは、次のような変形も可能である。

（１）ユーザが識別情報を記憶する代わりに、初期設定時に、ユーザが設定登録した識別情報を、サービスサーバを含む携帯電話機以外のサーバ30で記録し、相互認証時に、携帯電話機20がサーバ30からこの識別情報を読み出すようにしても良い。この場合、サーバ30は、設定登録された識別情報を携帯電話機20の電話番号と対応付けて格納する。携帯電話機20は、メモリデバイス10との相互認証時に、サーバ30に電話番号を通知し、該当する識別情報を取得してキーを生成する。こうすることで、ユーザは識別情報を頭で覚えている必要が無くなるため、入力ミスによる認証の失敗が無くなる。さらに初期設定時に、識別情報をユーザが設定登録するのではなく、アプリケーション22がこれを生成して、サーバに送信し、サーバがこれを登録するようにすれば、ユーザに識別情報を知られることが無くなり、ユーザ自身の不正操作によるメモリデバイス10への不正アクセスを排除することができる。

【 0 0 3 4 】

（２）初期設定時に、ユーザが設定登録した識別情報を外部メモリに格納し、ユーザは、この外部メモリを携帯電話機20と別に持ち歩く。ユーザは、機器認証時に、この外部メモリを携帯電話機20に装着し、アプリケーション22は、この外部メモリから識別情報を読み出して、相互認証時のキー生成を行う。外部メモリとしては、非接触型 I C カード、接触型 I C カード、S D カード、MMC カード等を用いることができる。

【 0 0 3 5 】

(3) 初期設定時に、携帯電話機20は、ユーザが保持する外部機器と通信し、この外部機器に識別情報を格納させる。機器認証時に、アプリケーション22は、携帯電話機20を通じて、この外部機器と通信し、識別情報を取得してキーを生成し、機器認証を行う。この外部機器としては、携帯電話、PDAなどが考えられ、また、携帯電話機20と外部機器との通信手段として、赤外線、Bluetoothなどが考えられる。この場合、ユーザが機器認証を行う携帯電話機20の近傍にこの外部機器を保持していれば、通信手段を通じて、外部機器から識別情報が携帯電話機20に読み出されて、機器認証が行われる。

【 0 0 3 6 】

(4) また、識別情報を暗号化して携帯電話機20内に格納し、この識別情報を復合化する複合鍵を前記(1)～(3)に示すように、サービスサーバ30、外部メモリ、あるいは、外部機器で保持するようにしてもよい。

(5) メモリデバイスへのキーの初期設定をオンラインで行う代わりに、メモリデバイスの発行元が、キーを予め埋め込んだメモリデバイスを発行するようにしても良い。この場合、ユーザは、携帯電話機の製造番号と識別情報とをメモリデバイス発行元に電話連絡し、あるいは、メモリデバイス発行元店頭で携帯電話機の製造番号と識別情報とを示してメモリデバイスの発行を申請する。メモリデバイス発行元は、それらの情報からキーを生成し、このキーを埋め込んだメモリデバイスをユーザに発行する。

【 0 0 3 7 】

また、実施形態では、セキュア領域を有しない携帯電話機と、セキュア領域を有するメモリデバイスとの相互認証について説明したが、相互認証の対象機器はそれだけに限らない。

例えば、ネット家電とこの機器に装着するメモリデバイスとの相互認証に対しても本発明を適用することができる。この場合、サービスサーバ30の役割は、各ネット家電と接続するホームサーバが担うことになる。このシステムでは、前記変形例(1)に示すように、ホームサーバが各ネット家電に対する識別情報を集中管理し、各ネット家電が、メモリデバイスとの相互認証時にホームサーバから該当する識別情報を取得するように構成することが効率的である。

また、セキュア領域を有する機器は、メモリデバイスだけで無く、耐タンパ性領域を有する機器であれば良い。

【 0 0 3 8 】

【発明の効果】

以上の説明から明らかなように、本発明の機器認証システム及び機器認証方法では、セキュアな領域を持たない機器を相手とする認証を安全確実に行うことができる。

また、これをメモリデバイスと携帯電話機との相互認証に適用する場合には、メモリデバイスに蓄積されたデータの利用を特定の携帯電話機だけに限定することができる。

【図面の簡単な説明】

【図 1】

本発明の実施形態における機器認証システムの構成を示す図

【図 2】

本発明の実施形態における機器認証システムでの初期設定手順を示す図

【図 3】

本発明の実施形態における機器認証システムでの相互認証手順を示す図

【図 4】

本発明の実施形態における機器認証システムでのメモリデバイスの一構成例を示す図

【図 5】

本発明の実施形態における機器認証システムでの携帯電話機の一構成例を示す図

【符号の説明】

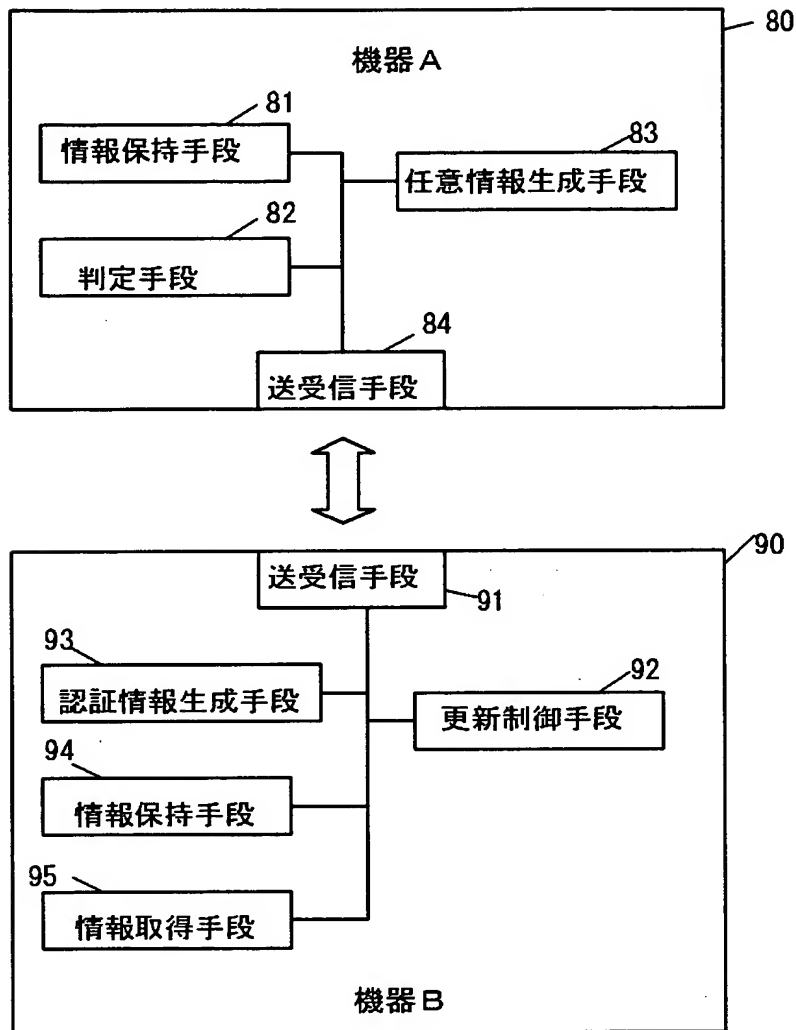
- 10 メモリデバイス
- 11 サーバ公開鍵
- 12 キー
- 13 メモリデバイス秘密鍵
- 20 携帯電話機

- 30 サービスサーバ
- 31 キャリアGW
- 41 メモリ
- 42 メモリコントローラ
- 43 CPU
- 44 RAM
- 45 ROM
- 46 内部不揮発性メモリ
- 47 暗号コプロセッサ
- 48 I/O部
- 49 I/O部
- 51 メモリデバイススロット
- 52 CPU
- 53 ROM
- 54 EEPROM
- 55 LCD
- 56 アンテナ
- 57 無線通信部
- 58 マイク
- 59 スピーカ
- 60 音声処理部
- 61 スイッチ
- 62 キー制御部
- 80 機器A
- 81 情報保持手段
- 82 判定手段
- 83 任意情報生成手段
- 84 送受信手段
- 90 機器B

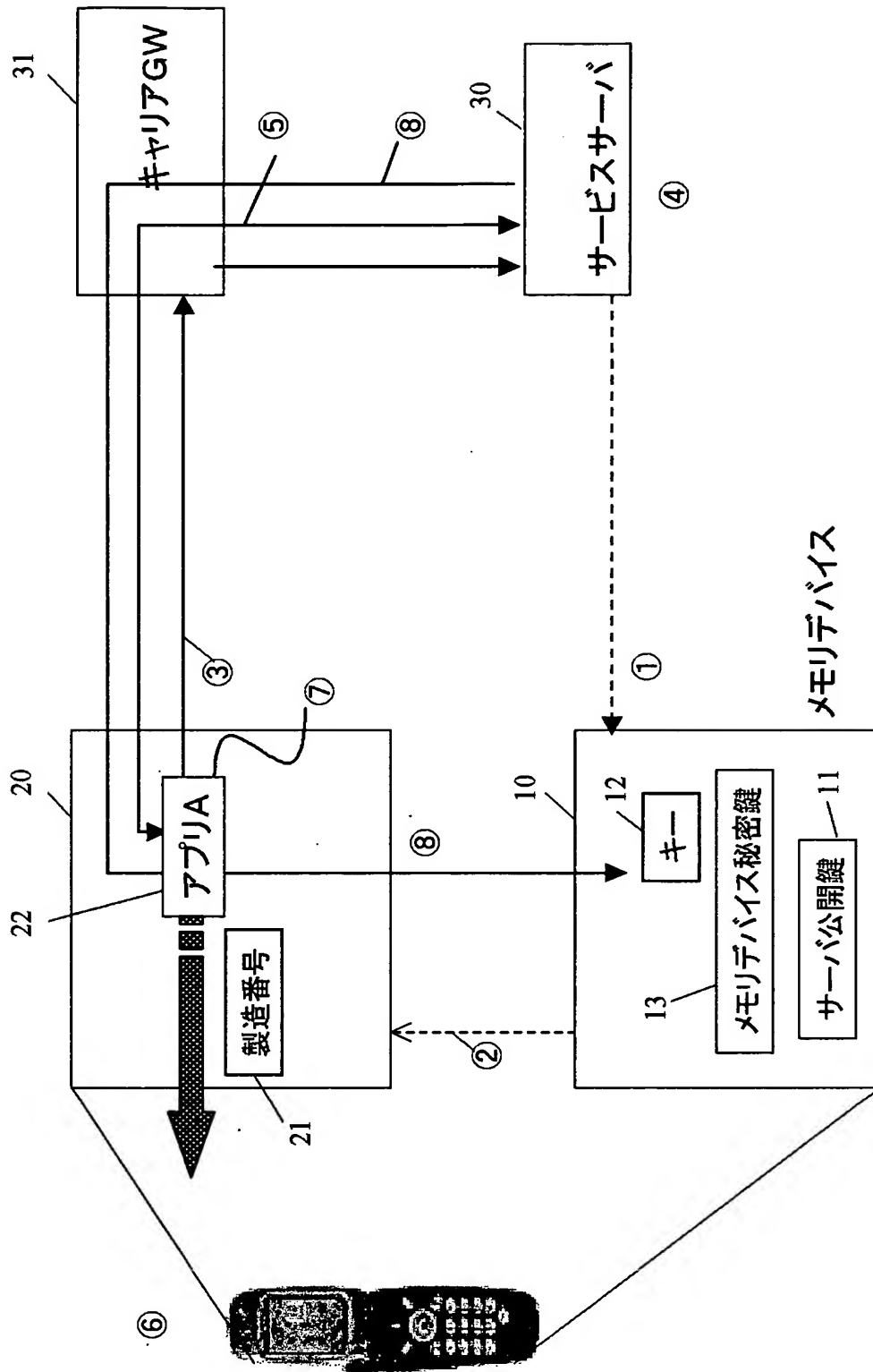
- 91 送受信手段
- 92 更新制御手段
- 93 認証情報生成手段
- 94 情報保持手段
- 95 情報取得手段

【書類名】 図面

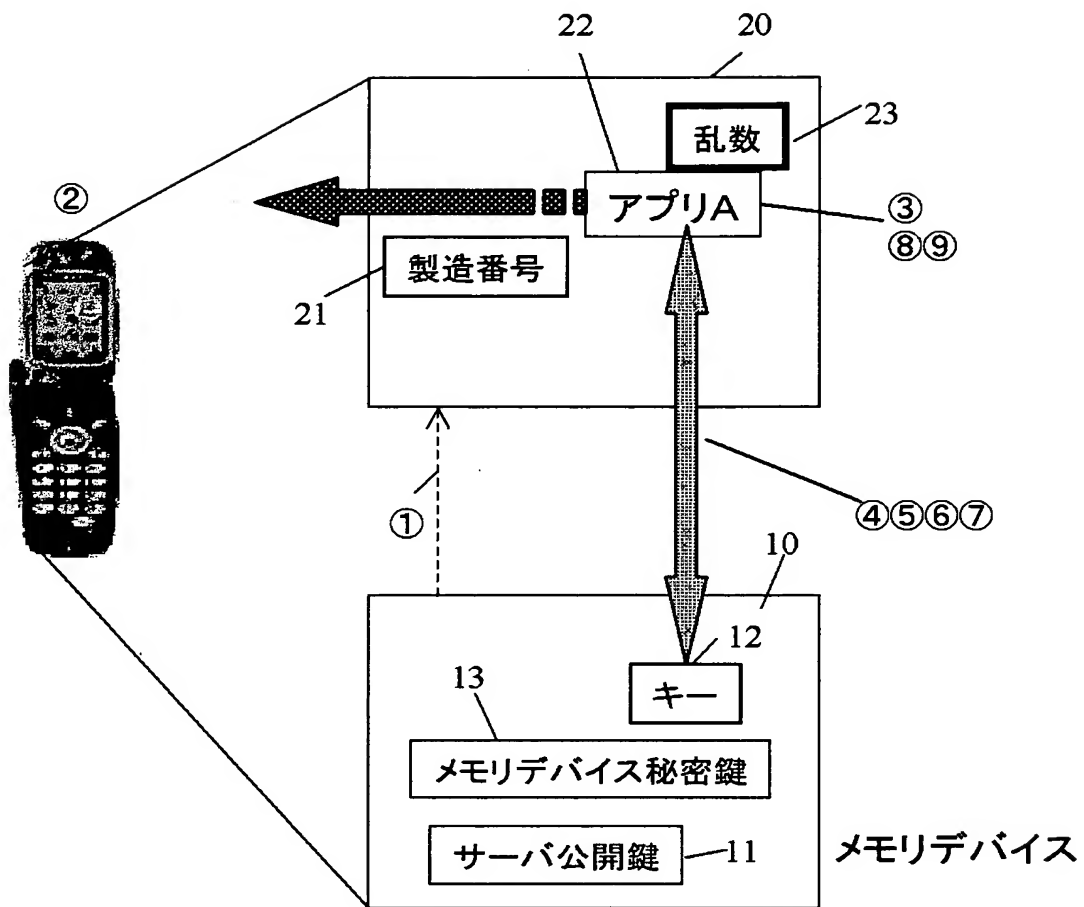
【図 1】



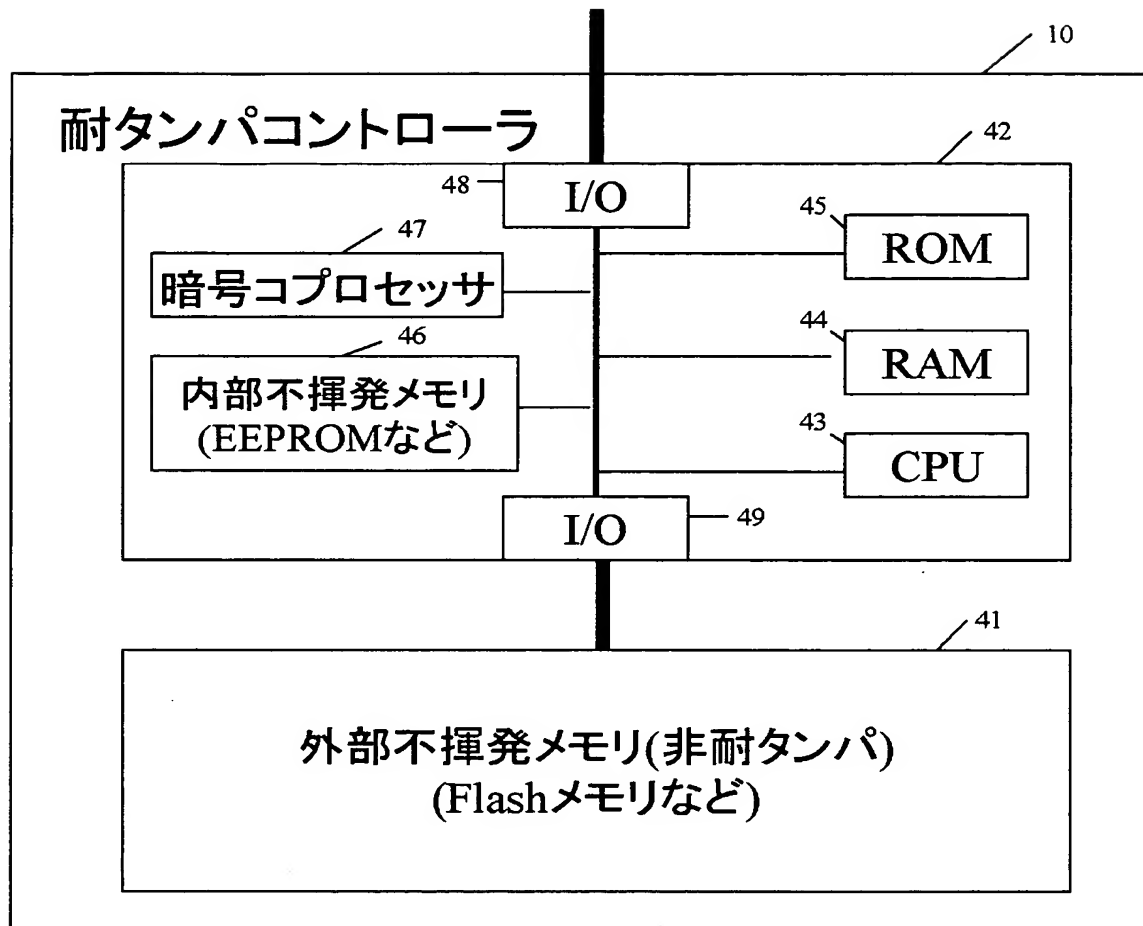
【図2】



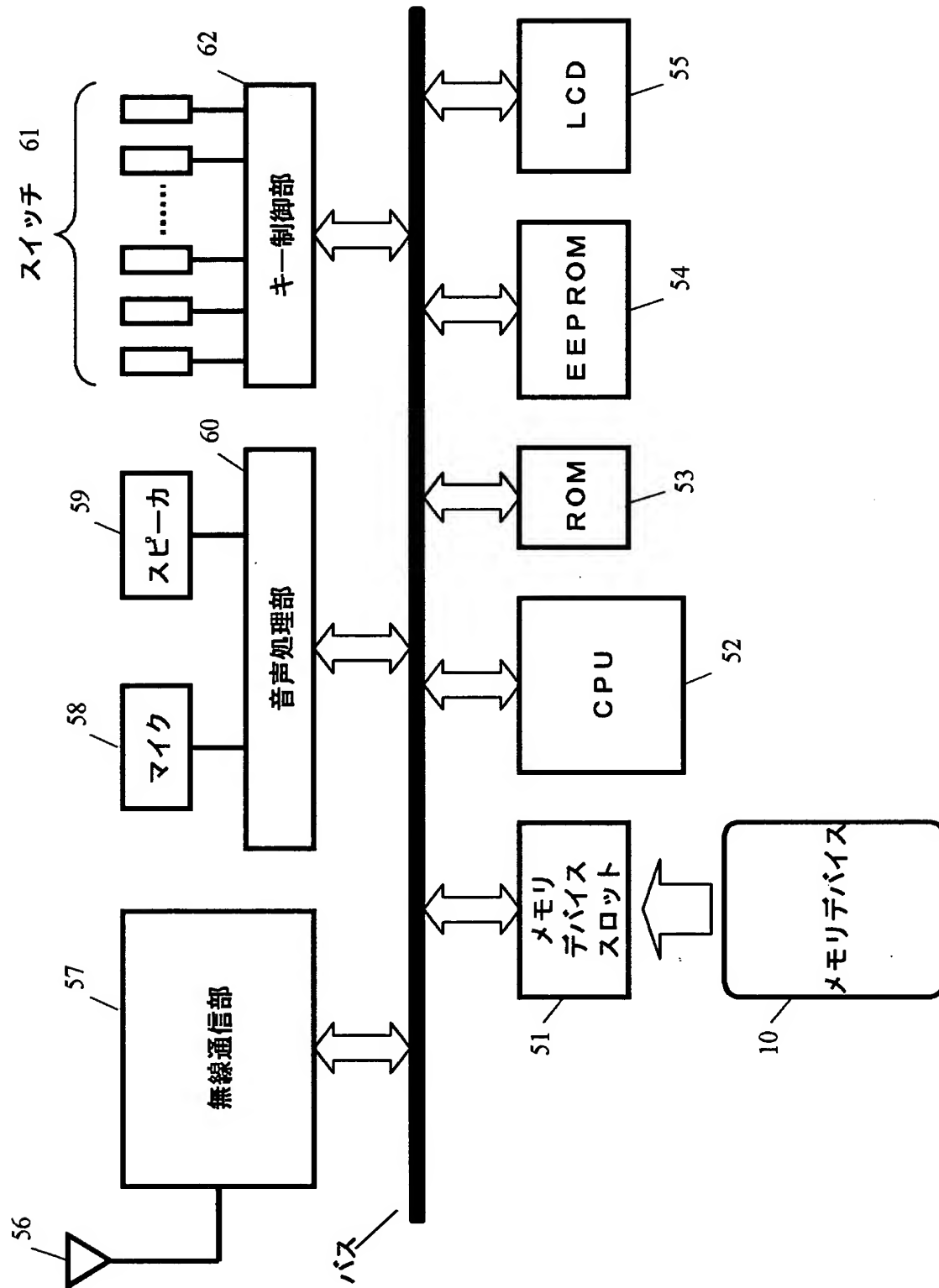
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 セキュアな領域を持たない機器を相手とする認証を安全確実に行うことができる機器認証システムを提供する。

【解決手段】 メモリデバイス10が携帯電話20を認証する機器認証システムにおいて、メモリデバイス10は、キー12をセキュアな領域に保持し、携帯電話20は、製造番号21を保持し、この製造番号とユーザから与えられる識別情報とからキーを生成し、メモリサーバ10は、保持するキー12と携帯電話20が生成したキーとの適合判定により、携帯電話20を認証する。この認証処理により、メモリデバイス10に蓄積されたデータの利用を特定の携帯電話機だけに限定することができる。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社